LA TUTELA DEI MINORI NON DEVE DIVENTARE IL GRIMALDELLO PER ELIMINARE LA LIBERTA' DI MANIFESTAZIONE DEL PENSIERO

La lotta contro gli abusi sessuali sui minori è un obiettivo legittimo e prioritario dell'Unione europea e degli Stati membri. Nessuno può contestarlo. Ciò che si contesta, e che deve essere contestato con forza giuridica, è il metodo: l'introduzione di meccanismi di scansione generalizzata e indiscriminata delle comunicazioni private (anche solo "volontaria" da parte dei fornitori di servizi) come strumento ordinario di contrasto al CSAM. Tale approccio, incarnato dal Regolamento (UE) 2021/1232 (deroga temporanea all'ePrivacy Directive, recentemente prorogata) e dalla più ampia proposta di Regolamento CSA (c.d. Chat Control 2.0), non può prevalere sulla libertà di espressione.
La libertà di espressione non è un diritto residuale da bilanciare all'infinito: essa costituisce uno dei pilastri di ogni società democratica e non può essere sacrificata sull'altare di una sorveglianza di massa tecnicamente fallibile e giuridicamente sproporzionata.

I. QUADRO NORMATIVO DI RIFERIMENTO CONTESTATO

Il Regolamento (UE) 2021/1232 ha introdotto una deroga temporanea e strettamente limitata agli articoli 5 e 6 della Direttiva 2002/58/CE, la direttiva ePrivacy, consentendo ai fornitori di servizi di comunicazione interpersonale indipendenti dal numero di effettuare, su base volontaria e nei limiti dello stretto necessario, il trattamento di dati personali e di altro tipo per rilevare e segnalare materiale di abuso sessuale su minori online e fenomeni di adescamento.

La proroga di tale regime, intervenuta nel luglio 2026 nonostante una maggioranza di voti contrari in Parlamento europeo (grazie a un meccanismo procedurale di maggioranza assoluta), prolunga fino al 2028 la possibilità di scansione delle comunicazioni non crittografate end-to-end. Parallelamente, i negoziati sul regolamento permanente (CSA Regulation) continuano a confrontarsi con il nodo della scansione obbligatoria o di obblighi di mitigazione del rischio talmente ampi da spingere di fatto verso forme di controllo generalizzato. Queste misure interferiscono direttamente con il contenuto delle comunicazioni private, non solo con i metadati.

Gli articoli 7 e seguenti della proposta di Regolamento CSAM (COM (2022) 209 final) disciplinano gli ordini di rilevazione. L'articolo 10 prevede che i fornitori di servizi di hosting e di comunicazione interpersonale che abbiano ricevuto un ordine di rilevazione lo eseguano installando e operando tecnologie per rilevare la diffusione di materiale di abuso sessuale su minori noto o nuovo, o la sollecitazione di minori, utilizzando gli indicatori forniti dal Centro UE.
Questo può comportare, nella pratica, la scansione sistematica delle comunicazioni, anche cifrate.
Queste misure interferiscono direttamente con il contenuto delle comunicazioni private, non solo con i metadati.

La Direttiva ePrivacy (2002/58/CE), all'articolo 5, paragrafo 1, stabilisce: «Gli Stati membri garantiscono la riservatezza delle comunicazioni e dei relativi dati sul traffico effettuati mediante una rete pubblica di comunicazioni e servizi di comunicazione elettronica accessibili al pubblico. In particolare, vietano l'ascolto, l'intercettazione, la memorizzazione o altre forme di intercettazione o di sorveglianza delle comunicazioni e dei relativi dati sul traffico da parte di persone diverse dagli utenti, senza il consenso degli utenti interessati, salvo quando sia legalmente autorizzato a norma dell'articolo 15, paragrafo 1.»

I diritti fondamentali coinvolti

La **Carta dei diritti fondamentali dell'Unione europea** tutela:

- **Articolo 7 – rispetto della vita privata e familiare, comprensivo della riservatezza delle comunicazioni**: «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.»;

- **Articolo 8 – protezione dei dati di carattere personale**: «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona

interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.»

- **Articolo 11 – libertà di espressione e d'informazione:** «1. Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. 2. La libertà dei media e il loro pluralismo sono rispettati.»

Questi articoli, letti congiuntamente, tutelano la segretezza tecnica e sostanziale delle comunicazioni, inclusa la crittografia end-to-end.

La **Convenzione europea dei diritti dell'uomo** tutela:

- **Articolo 8 – diritto al rispetto della vita privata e familiare e della corrispondenza**: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.»

- **Articolo 10 – libertà di espressione:** «1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.»

- L'articolo 52, paragrafo 1, della Carta impone che ogni limitazione di questi diritti sia prevista dalla legge, rispetti il contenuto essenziale dei diritti e sia proporzionata, necessaria e risponda a obiettivi di interesse generale. La scansione generalizzata delle comunicazioni private tocca l'essenza dei diritti di cui agli articoli 7 e 8 della Carta. Quando tale scansione produce un effetto dissuasivo sulla comunicazione libera, essa viola altresì l'articolo 11 della Carta e l'articolo 10 della CEDU.

La giurisprudenza della Corte di giustizia dell'Unione europea

La Corte di giustizia ha ripetutamente sancito che misure di sorveglianza generalizzata e indiscriminata sono incompatibili con la Carta.

Nella sentenza **Digital Rights Ireland** (cause riunite C-293/12 e C-594/12, 8 aprile 2014), la Corte ha dichiarato invalida la Direttiva 2006/24/CE sulla conservazione dei dati perché comportava un'ingerenza particolarmente grave nei diritti degli articoli 7 e 8 della Carta, non circoscritta a quanto strettamente necessario. La conservazione generalizzata di dati di traffico e di ubicazione consente di trarre conclusioni molto precise sulla vita privata delle persone. La conservazione generalizzata e indifferenziata di tutti i dati di traffico e di localizzazione costituisce un'ingerenza di vasta portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, non limitata allo stretto necessario e priva di garanzie sufficienti contro gli abusi.

Nella sentenza **Tele2 Sverige e Watson** (cause riunite C-203/15 e C-698/15, 21 dicembre 2016), la Corte ha affermato che l'articolo 15, paragrafo 1, della direttiva ePrivacy, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, osta a una normativa nazionale che preveda la conservazione generalizzata e indifferenziata di tutti i dati relativi al traffico e all'ubicazione di tutti gli abbonati e utenti registrati. Solo una conservazione mirata, limitata a quanto strettamente necessario per la lotta contro la criminalità grave, può essere ammissibile, e l'accesso deve essere soggetto a controllo preventivo di un'autorità giudiziaria o amministrativa indipendente.

Nella sentenza **La Quadrature du Net e a.** (cause riunite C-511/18, C-512/18 e C-520/18, 6 ottobre 2020), la Corte ha ribadito i limiti alla conservazione generalizzata e ha precisato le condizioni restrittive in cui possono essere ammesse misure di analisi automatizzata o di accesso in tempo reale.

Una conservazione generalizzata e indifferenziata dei dati di traffico e di localizzazione costituisce un'ingerenza particolarmente grave, giustificabile solo in presenza di una minaccia grave per la sicurezza nazionale che sia reale e attuale o prevedibile, e a condizioni rigorosamente delimitate. La lotta al materiale di abuso sessuale su minori, pur di primaria importanza, non rientra di per sé nella nozione di sicurezza nazionale.

Nella sentenza Schrems II (cause riunite C-311/18, C-512/18 e C-520/18, 6 ottobre 2020), la Corte ha affermato che una normativa che consente alle autorità pubbliche di accedere in modo generalizzato al contenuto delle comunicazioni elettroniche viola l'essenza del diritto al rispetto della vita privata. Queste decisioni non riguardano solo i metadati: esse stabiliscono un principio generale di divieto della sorveglianza di massa non mirata. La scansione del contenuto delle comunicazioni private è, se possibile, ancora più invasiva.

La giurisprudenza della Corte europea dei diritti dell'uomo

La Corte di Strasburgo ha sviluppato principi analoghi e, su alcuni punti, ancora più stringenti.
Nella sentenza della Grande Camera Big Brother Watch e altri c. Regno Unito, ricorsi n. 58170/13, 62322/14 e 24960/15 del 25 maggio 2021, la Corte ha accertato la violazione degli articoli 8 e 10 della Convenzione in relazione a regimi di intercettazione bulk e di acquisizione di dati di comunicazione. In particolare, ha sottolineato l'insufficiente protezione del materiale giornalistico confidenziale e l'effetto dissuasivo che regimi di sorveglianza di massa producono sulla libertà di stampa e di espressione. La Corte ha richiamato che la protezione delle fonti giornalistiche è uno dei pilastri della libertà di stampa e che qualsiasi ingerenza deve essere giustificata da un'esigenza prevalente di interesse pubblico.

La sorveglianza di massa deve essere circondata da garanzie particolarmente rigorose, pena il rischio di compromettere la democrazia stessa. La consapevolezza di essere potenzialmente soggetti a sorveglianza può produrre un effetto deterrente sull'esercizio della libertà di espressione.

Nella sentenza Podchasov c. Russia, ricorso n. 33696/19 del 13 febbraio 2024, la Corte ha dichiarato che l'obbligo imposto ai fornitori di servizi di comunicare chiavi di decrittazione o di indebolire la crittografia end-to-end viola l'articolo 8 della Convenzione.

La Corte ha esplicitamente riconosciuto che, nell'era digitale, le soluzioni tecniche di protezione della riservatezza delle comunicazioni elettroniche, inclusa la crittografia, contribuiscono a garantire il godimento di altri diritti fondamentali, in particolare la libertà di espressione. Indebolire la crittografia per tutti gli utenti al fine di consentire l'accesso alle comunicazioni di alcuni è sproporzionato e non necessario in una società democratica. Nella sentenza Szabó e Vissy c. Ungheria del 2016, la Corte ha affermato che un sistema di sorveglianza segreta non sufficientemente circoscritto può condurre ad abusi e violare sistematicamente l'articolo 8 della Convenzione.

Questi principi sono pienamente applicabili al Chat Control: la scansione generalizzata, anche se "volontaria" e limitata a contenuti noti di materiale di abuso sessuale su minori, crea un'infrastruttura di controllo permanente che produce un effetto dissuasivo sulla comunicazione libera, colpisce potenzialmente giornalisti, whistleblower, attivisti, persone LGBTQ+ in contesti ostili e chiunque dialoghi su temi sensibili.

La giurisprudenza della Corte europea dei diritti dell'uomo

La Corte di Strasburgo ha sviluppato principi analoghi e, su alcuni punti, ancora più stringenti.

Nella sentenza della Grande Camera **Big Brother Watch e altri c. Regno Unito** (ricorsi n. 58170/13, 62322/14 e 24960/15, 25 maggio 2021), la Corte ha accertato la violazione degli articoli 8 e 10 CEDU in relazione a regimi di intercettazione bulk e di acquisizione di dati di comunicazione. Ha sottolineato l'insufficiente protezione del materiale giornalistico confidenziale e l'effetto dissuasivo che regimi di sorveglianza di massa producono sulla libertà di stampa e di espressione. La protezione delle fonti giornalistiche è uno dei pilastri della libertà di stampa e qualsiasi ingerenza deve essere giustificata da un'esigenza prevalente di interesse pubblico.

La sorveglianza di massa deve essere circondata da garanzie particolarmente rigorose, pena il rischio di compromettere la democrazia stessa.

Nella sentenza **Podchasov c. Russia** (ricorso n. 33696/19, 13 febbraio 2024), la Corte ha dichiarato che l'obbligo imposto ai fornitori di servizi di comunicare chiavi di decrittazione o di indebolire la crittografia end-to-end viola l'articolo 8 CEDU. La Corte ha esplicitamente riconosciuto che, nell'era digitale, le soluzioni tecniche di protezione della riservatezza delle comunicazioni elettroniche, inclusa la crittografia, contribuiscono a garantire il godimento di altri diritti fondamentali, in particolare la libertà di espressione. Indebolire la crittografia per tutti gli utenti al fine di consentire l'accesso alle comunicazioni di alcuni è sproporzionato e non necessario in una società democratica.

Nella sentenza **Szabó e Vissy c. Ungheria** (2016), la Corte ha affermato che un sistema di sorveglianza segreta non sufficientemente circoscritto può condurre ad abusi e violare sistematicamente l'articolo 8 della Convenzione.
Questi principi sono pienamente applicabili al Chat Control: la scansione generalizzata, anche se "volontaria" e limitata a contenuti noti di CSAM, crea un'infrastruttura di controllo permanente che produce un effetto dissuasivo sulla comunicazione libera, colpisce potenzialmente giornalisti, whistleblower, attivisti, persone LGBTQ+ in contesti ostili e chiunque dialoghi su temi sensibili.

Sulla pretesa proporzionalità e necessità e sull'applicazione dei principi alla proposta di Regolamento CSAM

I sostenitori del Chat Control affermano che la scansione è necessaria e proporzionata perché mira a proteggere i minori. Tale argomento non regge al vaglio giuridico.
La giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo esige che le misure interferenti con i diritti fondamentali siano strettamente necessarie e non vadano oltre quanto richiesto dall'obiettivo. Misure mirate, basate su un sospetto concreto, autorizzate da un'autorità giudiziaria e soggette a garanzie procedurali rigorose, esistono già e sono pienamente compatibili con il diritto dell'Unione e con la Convenzione europea dei diritti dell'uomo.
La scansione di massa non è l'unica, né la più efficace, né la meno invasiva delle opzioni possibili.

Inoltre, i tassi di falsi positivi delle tecnologie di rilevamento automatico – anche elevati secondo valutazioni della Commissione stessa –, il rischio di errori di classificazione, la possibilità di abusi futuri e l'effetto dissuasivo sulla comunicazione privata rendono la misura strutturalmente sproporzionata.

- La scansione delle chat è una forma di intercettazione preventiva. Il client-side scanning analizza il contenuto dei messaggi, le immagini, i video e i metadati prima ancora che la comunicazione sia cifrata. È, tecnicamente e giuridicamente, intercettazione del contenuto.

- La misura è generalizzata e indiscriminata. Gli ordini di rilevazione previsti dalla proposta:
  - si applicano a interi servizi e, di fatto, a tutti gli utenti di tali servizi;
  - analizzano le comunicazioni in modo sistematico;
  - prescindono da qualsiasi sospetto individuale.

Sono strutturalmente assimilabili alla conservazione generalizzata dei dati già dichiarata incompatibile con il diritto dell'Unione dalla Corte di giustizia.

- Violano l'essenza dei diritti fondamentali. Come affermato in Schrems II, l'accesso generalizzato al contenuto delle comunicazioni viola l'essenza del diritto al rispetto della vita privata. Nella proposta non si tratta soltanto di accesso, ma di analisi automatica obbligatoria del contenuto.

- Producono un effetto di autocensura. La Corte europea dei diritti dell'uomo ha riconosciuto che la sorveglianza dissuade dall'esercizio della libertà di espressione. Gli utenti, sapendo che ogni messaggio può essere analizzato, evitano contenuti sensibili, discussioni delicate ed espressioni legittime ma potenzialmente fraintese dagli algoritmi.

- Non rispettano il principio di proporzionalità di cui all'articolo 52 della Carta. Una misura è proporzionata solo se è necessaria – non esistono alternative meno intrusive –, idonea e non lesiva dell'essenza del diritto. Esistono alternative meno intrusive: indagini mirate, cooperazione internazionale, rimozione rapida dei contenuti segnalati, strumenti volontari ed educazione digitale. La scansione sistematica e generalizzata non è necessaria.

La libertà di espressione non può essere ridotta a un diritto di secondo rango. Un sistema che induce i cittadini a censurarsi preventivamente per paura di essere scansionati, segnalati o investigati non è un sistema democratico: è un sistema di controllo.

Il ruolo delle ONG nel dibattito sul Regolamento CSAM

Il ruolo delle organizzazioni non governative nel dibattito è polarizzato e strutturalmente diviso in due blocchi principali, che esercitano un'influenza significativa sulle istituzioni europee attraverso lobbying, lettere aperte, campagne pubbliche e produzione di dati e rapporti. Queste organizzazioni non sono attori neutrali: agiscono come moltiplicatori di pressione politica e tecnica.

Il blocco delle ONG di protezione dei minori *(ECLAG – European Child Sexual Abuse Legislation Advocacy Group, che riunisce oltre 70-80 organizzazioni tra cui ECPAT International, Eurochild, Missing Children Europe, Internet Watch Foundation, Terre des Hommes Netherlands e Thorn; WeProtect Global Alliance e altre coalizioni)* sostiene strumenti di rilevamento proattivo, anche obbligatori, ritenendo insufficienti le sole indagini mirate. Sottolinea l'aumento dei contenuti generati con intelligenza artificiale e chiede un quadro legislativo ambizioso e stabile.

ECLAG (European Child Sexual Abuse Legislation Advocacy Group): coalizione di oltre 70-80 organizzazioni per i diritti dell'infanzia (include ECPAT International, Eurochild, Missing Children Europe, Internet Watch Foundation, Terre des Hommes Netherlands e Thorn).
Ha espresso ripetutamente delusione per le posizioni del Parlamento che limitano o interrompono le misure di rilevamento, definendole "inaccettabili" perché creano "vuoti di protezione".
Chiede ambizione normativa, estensione della deroga temporanea e un regolamento permanente robusto, sottolineando l'aumento dei contenuti AI-generati e la necessità di continuità operativa per i provider.

Thorn: ONG statunitense fondata da Ashton Kutcher e Demi Moore. Sviluppa tecnologie di rilevamento (prodotto "Safer") e fa lobbying intensivo a Bruxelles (incontri documentati con gabinetti della Commissione, inclusa quello di von der Leyen e della commissaria Johansson). Collabora con Google, Intel e Palantir. Ha chiesto certezza giuridica per la scansione proattiva e un Centro UE operativo.

WeProtect Global Alliance: rete internazionale che riunisce governi, organizzazioni e aziende. È citata positivamente dalla Commissione europea nella propria strategia e ha partecipato a discussioni strategiche e a finanziamenti europei.

Altre coalizioni: oltre 100 organizzazioni per i diritti dei bambini hanno firmato lettere aperte (2026) per sollecitare un quadro legislativo ambizioso, sostenendo che senza obblighi di rilevamento le piattaforme non agiscono in modo adeguato e che i cittadini europei supportano in maggioranza misure di questo tipo.

Argomenti tipici di questo blocco: la scansione (anche volontaria) ha permesso di identificare e soccorrere vittime; l'interruzione della base giuridica (come avvenuto temporaneamente nel 2026) ha portato a cali significativi delle segnalazioni (es. -58% verso il NCMEC secondo alcune stime); le alternative "solo mirate" lasciano scoperte le piattaforme a rischio. Queste ONG collaborano spesso con autorità di contrasto e forniscono banche dati di indicatori CSAM.

Il blocco delle ONG di diritti digitali e libertà civili *(EDRi e organizzazioni affiliate, Global Encryption Coalition – che include Centre for Democracy & Technology Europe, Internet Society, Mozilla, Global Partners Digital e Internet Freedom Foundation – nonché campagne come Fight*

Chat Control e lettere di oltre 80 gruppi) si oppone fermamente a qualsiasi forma di scansione indiscriminata o quasi-indiscriminata delle comunicazioni private, anche se "volontaria".
Ritiene tale misura incompatibile con gli articoli 7, 8 e 11 della Carta e con la giurisprudenza consolidata della Corte di giustizia e della Corte EDU, e propone invece misure mirate, giudiziarie e di prevenzione.

Questa polarizzazione ha contribuito a rendere il dossier uno dei più lunghi e contenziosi della legislatura europea, con proroghe successive della deroga 2021/1232 e negoziati ancora aperti sul regolamento permanente.

EDRi (European Digital Rights) e organizzazioni affiliate: critica sistematica della proporzionalità, dei falsi positivi elevati e dell'effetto dissuasivo sulla libertà di espressione. Ha coordinato o sostenuto lettere aperte (oltre 40 organizzazioni nel 2026) contro ulteriori proroghe della deroga ePrivacy, chiedendo esclusioni esplicite della scansione non mirata e limiti temporali stretti.

Global Encryption Coalition (include Centre for Democracy & Technology Europe, Internet Society, Mozilla, Global Partners Digital, Internet Freedom Foundation): ha accolto positivamente le posizioni del Consiglio che rimuovono obblighi di rilevamento obbligatorio sui servizi crittografati, ribadendo che indebolire la crittografia end-to-end danneggia tutti, minori inclusi.

Campagne e coalizioni più ampie: Fight Chat Control, lettere di oltre 80 gruppi (diritti digitali, difensori dei diritti umani, organizzazioni femminili e per l'infanzia critiche), CEPIS, AEGEE-Europe, Ecologistas en Acción e altre. Sottolineano l'assenza di prove di efficacia della scansione di massa sulle condanne o sui salvataggi, i tassi elevati di falsi positivi e il rischio di precedente autoritario.

Argomenti tipici di questo blocco: esistono alternative meno intrusive (indagini mirate con autorizzazione giudiziaria, cooperazione internazionale, rimozione rapida, prevenzione ed educazione); la scansione generalizzata viola l'essenza dei diritti fondamentali e produce autocensura; le tecnologie non sono affidabili e possono essere estese in futuro ad altri contenuti.

1. Modalità di influenza e criticità

- **Lobbying e accesso istituzionale**: entrambe le parti sono presenti nel Registro per la trasparenza dell'UE. Le ONG pro-protezione dei minori hanno avuto incontri diretti con alti funzionari della Commissione e beneficiano di reti come WeProtect. Le ONG di diritti digitali mobilizzano campagne di massa (email ai parlamentari, siti come fightchatcontrol.eu) e collaborano con esperti di crittografia e con aziende (Signal, Tuta, ecc.).

- **Produzione di evidenze**: le prime forniscono dati su volumi di CSAM e su cali di segnalazioni; le seconde evidenziano rapporti della Commissione sui falsi positivi e l'assenza di nesso dimostrabile tra scansione di massa e risultati investigativi concreti.

- **Polarizzazione e alleanze**: le ONG di protezione dei minori si allineano spesso con forze di polizia (Europol) e con parte dell'industria tech che offre strumenti di rilevamento. Le ONG di diritti digitali si allineano con esperti di sicurezza, alcune imprese europee e parte del Parlamento (soprattutto gruppi verdi/liberali/pirati).

In sintesi, le ONG non sono un attore monolitico: fungono da **catalizzatori di due visioni irriducibili**. Quelle orientate alla protezione dei minori spingono per strumenti di rilevamento ampi e stabili, ritenendo che senza di essi i minori restino esposti.
Quelle orientate ai diritti digitali e alla privacy considerano la scansione generalizzata (anche volontaria e "temporanea") una violazione strutturale dei diritti fondamentali e un precedente pericoloso, proponendo invece misure mirate, giudiziarie e di prevenzione.

Questa polarizzazione ha contribuito a rendere il dossier uno dei più lunghi e contenziosi della legislatura europea, con proroghe successive della deroga 2021/1232 e negoziati ancora aperti sul regolamento permanente. Il peso politico delle ONG deriva dalla loro capacità di fornire legittimazione morale, dati e pressione pubblica, ma anche dalla loro interconnessione con interessi tecnologici e istituzionali.

Conclusioni

Il Regolamento CSAM, nella sua versione attuale e in quella prospettata, non può sacrificare la libertà di espressione sull'altare di una sorveglianza generalizzata.

La giurisprudenza consolidata della Corte di giustizia (Digital Rights Ireland, Tele2/Watson, La Quadrature du Net, Schrems II) e della Corte europea dei diritti dell'uomo (Big Brother Watch, Podchasov, Szabó e Vissy) stabilisce limiti chiari e non negoziabili:

- *divieto di sorveglianza generalizzata e indiscriminata;*
- *tutela dell'essenza dei diritti di cui agli articoli 7, 8 e 11 della Carta;*
- *riconoscimento del ruolo della crittografia e della riservatezza delle comunicazioni come condizioni essenziali per l'esercizio della libertà di espressione;*
- *esigenza di misure mirate, proporzionate e sottoposte a controllo indipendente.*

Proteggere i minori e tutelare la libertà di espressione non sono obiettivi in contrasto. Sono obiettivi che devono e possono coesistere attraverso strumenti giuridici precisi, mirati e rispettosi dei diritti fondamentali. Qualsiasi deroga a questi principi deve essere respinta. La libertà di espressione non si negozia.

THE PROTECTION OF MINORS MUST NOT BECOME THE PRETEXT FOR ELIMINATING FREEDOM OF EXPRESSION

The fight against the sexual abuse of minors is a legitimate and priority objective of the European Union and its Member States. No one can contest this. What is contested, and what must be contested with legal force, is the method: the introduction of mechanisms for the generalised and indiscriminate scanning of private communications (even if only "voluntary" on the part of service providers) as an ordinary tool to combat CSAM. This approach, embodied in Regulation (EU) 2021/1232 (the temporary derogation from the ePrivacy Directive, recently extended) and in the broader proposal for a CSA Regulation (so-called Chat Control 2.0), cannot prevail over freedom of expression. Freedom of expression is not a residual right to be endlessly balanced: it constitutes one of the pillars of every democratic society and cannot be sacrificed on the altar of mass surveillance that is technically fallible and legally disproportionate.

I. THE CONTESTED REGULATORY FRAMEWORK

Regulation (EU) 2021/1232 introduced a temporary and strictly limited derogation from Articles 5 and 6 of Directive 2002/58/EC (the ePrivacy Directive), allowing providers of number-independent interpersonal communications services to process, on a voluntary basis and within the limits of what is strictly necessary, personal data and other data in order to detect and report online child sexual abuse material and grooming.

The extension of this regime, adopted in July 2026 despite a majority of votes against it in the European Parliament (thanks to a procedural absolute-majority mechanism), prolongs until 2028 the possibility of scanning non-end-to-end encrypted communications. In parallel, negotiations on the permanent regulation (CSA Regulation) continue to confront the issue of mandatory scanning or risk-mitigation obligations so broad as to push de facto towards forms of generalised control.
These measures interfere directly with the content of private communications, not merely with metadata.

Articles 7 et seq. of the proposed CSAM Regulation (COM(2022) 209 final) regulate detection orders. Article 10 provides that providers of hosting and interpersonal communications services that have received a detection order shall execute it by installing and operating technologies to detect the dissemination of known or new child sexual abuse material, or the solicitation of children, using the indicators provided by the EU Centre. This may, in practice, entail the systematic scanning of communications, including encrypted ones. These measures interfere directly with the content of private communications, not merely with metadata.

Article 5(1) of the ePrivacy Directive (2002/58/EC) states: "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)."

Fundamental rights engaged

The Charter of Fundamental Rights of the European Union protects:

- **Article 7 – Respect for private and family life, including the confidentiality of communications**: "Everyone has the right to respect for his or her private and family life, home and communications."

- **Article 8 – Protection of personal data**: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her,

and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

- **Article 11 – Freedom of expression and information**: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected."

Read together, these articles protect both the technical and the substantive secrecy of communications, including end-to-end encryption.

The European Convention on Human Rights protects:

- **Article 8 – Right to respect for private and family life and correspondence**: "1. Everyone has the right to respect for his private and family life, his home and his correspondence."

- **Article 10 – Freedom of expression**: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

- **Article 52(1) of the Charter requires that any limitation on these rights be provided for by law**, respect the essence of those rights and freedoms, and be proportionate, necessary and genuinely meet objectives of general interest. Generalised scanning of private communications touches the essence of the rights under Articles 7 and 8 of the Charter. When such scanning produces a chilling effect on free communication, it also violates Article 11 of the Charter and Article 10 ECHR.

Case-law of the Court of Justice of the European Union

The Court of Justice has repeatedly held that generalised and indiscriminate surveillance measures are incompatible with the Charter.

In ***Digital Rights Ireland*** (joined cases C-293/12 and C-594/12, 8 April 2014), the Court declared Directive 2006/24/EC on data retention invalid because it entailed a particularly serious interference with the rights under Articles 7 and 8 of the Charter that was not limited to what was strictly necessary. The generalised retention of traffic and location data makes it possible to draw very precise conclusions concerning the private lives of the persons concerned.
Generalised and undifferentiated retention of all traffic and location data constitutes an interference of wide scope and particular gravity with the fundamental rights to respect for private life and to the protection of personal data, which is not limited to what is strictly necessary and lacks sufficient safeguards against abuse.

In ***Tele2 Sverige and Watson*** (joined cases C-203/15 and C-698/15, 21 December 2016), the Court held that Article 15(1) of the ePrivacy Directive, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precludes national legislation providing for the generalised and undifferentiated retention of all traffic and location data of all subscribers and registered users. Only targeted retention, limited to what is strictly necessary for the purpose of fighting serious crime, may be permissible, and access must be subject to prior review by a court or an independent administrative authority.

In ***La Quadrature du Net and Others*** (joined cases C-511/18, C-512/18 and C-520/18, 6 October 2020), the Court reiterated the limits on generalised retention and clarified the restrictive conditions under which automated analysis measures or real-time access may be authorised. Generalised and undifferentiated retention of traffic and location data constitutes a particularly serious interference, justifiable only in the presence of a serious threat to national security that is genuine and present or

foreseeable, and under strictly delimited conditions. The fight against child sexual abuse material, although of primary importance, does not in itself fall within the concept of national security.

In ***Schrems II*** (Case C-311/18, 16 July 2020), the Court held that legislation permitting public authorities to have generalised access to the content of electronic communications infringes the essence of the right to respect for private life. These rulings do not concern metadata alone: they establish a general principle prohibiting non-targeted mass surveillance. Scanning the content of private communications is, if anything, even more intrusive.

Case-law of the European Court of Human Rights

The Strasbourg Court has developed analogous and, on certain points, even stricter principles.
In the Grand Chamber judgment *Big Brother Watch and Others v. the United Kingdom* (applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021), the Court found violations of Articles 8 and 10 of the Convention in relation to bulk interception regimes and the acquisition of communications data. It emphasised the insufficient protection of confidential journalistic material and the chilling effect that mass-surveillance regimes produce on freedom of the press and expression. The Court recalled that the protection of journalistic sources is one of the cornerstones of freedom of the press and that any interference must be justified by an overriding requirement in the public interest.

Mass surveillance must be surrounded by particularly rigorous safeguards, otherwise there is a risk of undermining democracy itself. The awareness of being potentially subject to surveillance may produce a deterrent effect on the exercise of freedom of expression.

In *Podchasov v. Russia* (application no. 33696/19, 13 February 2024), the Court held that the obligation imposed on service providers to disclose decryption keys or to weaken end-to-end encryption violates Article 8 of the Convention.

The Court expressly recognised that, in the digital age, technical solutions for protecting the confidentiality of electronic communications, including encryption, contribute to ensuring the enjoyment of other fundamental rights, in particular freedom of expression. Weakening encryption for all users in order to enable access to the communications of some is disproportionate and not necessary in a democratic society.

In *Szabó and Vissy v. Hungary* (2016), the Court held that a secret surveillance system that is not sufficiently circumscribed may lead to abuse and systematically violate Article 8 of the Convention. These principles are fully applicable to Chat Control: generalised scanning, even if "voluntary" and limited to known child sexual abuse material, creates a permanent control infrastructure that produces a chilling effect on free communication and potentially affects journalists, whistle-blowers, activists, LGBTQ+ persons in hostile environments, and anyone discussing sensitive topics.

On the alleged proportionality and necessity and the application of the principles to the proposed CSAM Regulation

Supporters of Chat Control claim that scanning is necessary and proportionate because it aims to protect minors. This argument does not withstand legal scrutiny.
The case-law of the Court of Justice and the European Court of Human Rights requires that measures interfering with fundamental rights be strictly necessary and go no further than required by the objective. Targeted measures, based on concrete suspicion, authorised by a judicial authority and subject to rigorous procedural safeguards, already exist and are fully compatible with Union law and the European Convention on Human Rights. Mass scanning is neither the only, nor the most effective, nor the least intrusive of the available options. Moreover, the false-positive rates of automatic detection technologies — which are high even according to the Commission's own assessments — the risk of misclassification, the possibility of future abuse, and the chilling effect on private communication render the measure structurally disproportionate.

- Chat scanning is a form of preventive interception. Client-side scanning analyses the content of messages, images, videos and metadata before the communication is even encrypted. It is, both technically and legally, interception of content.
- The measure is generalised and indiscriminate. The detection orders provided for in the proposal:
  - apply to entire services and, in practice, to all users of those services;
  - analyse communications systematically;
  - are independent of any individual suspicion.

They are structurally comparable to the generalised data retention already held incompatible with Union law by the Court of Justice.

- They violate the essence of fundamental rights. As held in *Schrems II*, generalised access to the content of communications violates the essence of the right to respect for private life. The proposal involves not merely access, but mandatory automatic analysis of content.

- They produce a self-censorship effect. The European Court of Human Rights has recognised that surveillance deters the exercise of freedom of expression. Users, knowing that every message may be analysed, avoid sensitive content, delicate discussions and legitimate expressions that may potentially be misinterpreted by algorithms.

- They fail to respect the principle of proportionality under Article 52 of the Charter. A measure is proportionate only if it is necessary — no less intrusive alternatives exist — suitable, and does not impair the essence of the right. Less intrusive alternatives exist: targeted investigations, international cooperation, rapid removal of reported content, voluntary tools and digital education. Systematic and generalised scanning is not necessary.

Freedom of expression cannot be reduced to a second-class right. A system that induces citizens to censor themselves preventively for fear of being scanned, reported or investigated is not a democratic system: it is a system of control.

The role of NGOs in the debate on the CSAM Regulation

The role of non-governmental organisations in the debate is polarised and structurally divided into two main blocs, which exert significant influence on the European institutions through lobbying, open letters, public campaigns and the production of data and reports. These organisations are not neutral actors: they act as multipliers of political and technical pressure.

The child-protection NGO bloc *(ECLAG – European Child Sexual Abuse Legislation Advocacy Group, which brings together more than 70–80 organisations including ECPAT International, Eurochild, Missing Children Europe, Internet Watch Foundation, Terre des Hommes Netherlands and Thorn; WeProtect Global Alliance and other coalitions)* supports proactive detection tools, including mandatory ones, considering targeted investigations alone insufficient. It highlights the rise in AI-generated content and calls for an ambitious and stable legislative framework.

ECLAG (European Child Sexual Abuse Legislation Advocacy Group): has repeatedly expressed disappointment at parliamentary positions that limit or interrupt detection measures, describing them as “unacceptable” because they create “protection gaps”. It calls for legislative ambition, extension of the temporary derogation and a robust permanent regulation, stressing the increase in AI-generated content and the need for operational continuity for providers.

Thorn (a US NGO founded by Ashton Kutcher and Demi Moore) develops detection technologies (the “Safer” product) and engages in intensive lobbying in Brussels. It has called for legal certainty for proactive scanning and an operational EU Centre.
WeProtect Global Alliance is an international network bringing together governments, organisations and companies. It is cited positively by the European Commission in its strategy.

Typical arguments of this bloc: scanning (even voluntary) has enabled the identification and rescue of victims; the temporary interruption of the legal basis (as occurred in 2026) led to significant drops in reports (e.g. –58 % to NCMEC according to some estimates); "targeted-only" alternatives leave at-risk platforms uncovered.

The digital-rights and civil-liberties NGO bloc (EDRi and affiliated organisations, the Global Encryption Coalition — which includes the Centre for Democracy & Technology Europe, Internet Society, Mozilla, Global Partners Digital and Internet Freedom Foundation — as well as campaigns such as Fight Chat Control and letters from more than 80 groups) firmly opposes any form of indiscriminate or quasi-indiscriminate scanning of private communications, even if "voluntary". It considers such a measure incompatible with Articles 7, 8 and 11 of the Charter and with the established case-law of the Court of Justice and the ECtHR, and instead proposes targeted, judicial and preventive measures.

This polarisation has contributed to making the dossier one of the longest and most contentious of the European legislative term, with successive extensions of the 2021/1232 derogation and negotiations still open on the permanent regulation.

EDRi (European Digital Rights) and affiliated organisations: systematic criticism of proportionality, high false-positive rates and the chilling effect on freedom of expression. It has coordinated or supported open letters (more than 40 organisations in 2026) against further extensions of the ePrivacy derogation, calling for explicit exclusions of non-targeted scanning and strict time limits.

Global Encryption Coalition (includes Centre for Democracy & Technology Europe, Internet Society, Mozilla, Global Partners Digital, Internet Freedom Foundation): welcomed the Council's positions removing mandatory detection obligations on encrypted services, reiterating that weakening end-to-end encryption harms everyone, including minors.

Broader campaigns and coalitions: Fight Chat Control, letters from more than 80 groups (digital rights organisations, human rights defenders, women's organisations and critical children's rights organisations), CEPIS, AEGEE-Europe, Ecologistas en Acción and others. They highlight the lack of evidence of the effectiveness of mass scanning in terms of convictions or rescues, the high rates of false positives, and the risk of an authoritarian precedent.

Typical arguments of this bloc: less intrusive alternatives exist (targeted investigations with judicial authorisation, international cooperation, rapid removal, prevention and education); generalised scanning violates the essence of fundamental rights and produces self-censorship; the technologies are unreliable and may be extended in the future to other types of content.

Modes of influence and critical aspects

- **Lobbying and institutional access**: both sides are registered in the EU Transparency Register. Child-protection NGOs have had direct meetings with senior Commission officials and benefit from networks such as WeProtect. Digital-rights NGOs mobilise mass campaigns (emails to Members of Parliament, websites such as fightchatcontrol.eu) and collaborate with encryption experts and companies (Signal, Tuta, etc.).

- **Production of evidence**: the former provide data on volumes of CSAM and on drops in reporting; the latter highlight Commission reports on false positives and the absence of a demonstrable link between mass scanning and concrete investigative outcomes.

- **Polarisation and alliances**: child-protection NGOs often align with law-enforcement authorities (Europol) and with parts of the tech industry that offer detection tools. Digital-rights NGOs align with security experts, certain European companies and parts of the Parliament (especially the Greens/liberals/pirates).

In summary, NGOs are not a monolithic actor: they act as catalysts for two irreconcilable visions. Those oriented towards the protection of minors push for broad and stable detection tools, believing that without them minors remain exposed. Those oriented towards digital rights and privacy regard generalised scanning (even if voluntary and "temporary") as a structural violation of fundamental rights and a dangerous precedent, proposing instead targeted, judicial and preventive measures.
This polarisation has contributed to making the dossier one of the longest and most contentious of the European legislative term, with successive extensions of the 2021/1232 derogation and negotiations still open on the permanent regulation. The political weight of the NGOs derives from their ability to provide moral legitimacy, data and public pressure, but also from their interconnections with technological and institutional interests.

Conclusions

The CSAM Regulation, in its current version and in the version envisaged, cannot sacrifice freedom of expression on the altar of generalised surveillance.
The established case-law of the Court of Justice (*Digital Rights Ireland*, *Tele2/Watson*, *La Quadrature du Net*, *Schrems II*) and of the European Court of Human Rights (*Big Brother Watch*, *Podchasov*, *Szabó and Vissy*) lays down clear and non-negotiable limits:

- *prohibition of generalised and indiscriminate surveillance;*
- *protection of the essence of the rights under Articles 7, 8 and 11 of the Charter;*
- *recognition of the role of encryption and of the confidentiality of communications as essential conditions for the exercise of freedom of expression;*
- *the requirement of targeted, proportionate measures subject to independent oversight.*

Protecting minors and protecting freedom of expression are not conflicting objectives. They are objectives that must and can coexist through precise, targeted legal instruments that respect fundamental rights. Any derogation from these principles must be rejected. Freedom of expression is not negotiable.